What is claimed is:

Sub A1

1. A works protecting system comprising an AV data transmitting-receiving device for transmitting contents of works and a transmitting-receiving device on another party for receiving the works,

wherein said AV data transmitting-receiving device comprises command input means, command control means, AV data transmitting means, encrypting means, first authenticating means, first input/output means, device ID detecting means, and authentication histories storing means,

wherein said transmitting-receiving device on another party comprises second input/output means, AV data receiving means, decrypting means, and second authenticating means, and

wherein said authenticating means performs a device authentication operation for mutually checking that both said devices are devices based on certain rules, and a key exchange operation for sharing a cryptographic key for simultaneously encrypting and decrypting the works when said transmitting-receiving device on another party with a history that authentication has been previously performed therefor is connected to a transmission line.

2. A works protecting system comprising an AV data transmitting-receiving device for transmitting contents of works and a plurality of transmitting-receiving devices on the other parties for receiving the works,

wherein said AV data transmitting-receiving device comprises command input means, command control means, AV data transmitting means, encrypting means, first authenticating means, first input/output means, device ID detecting means, authentication histories storing means, and cryptographic key storing means,

wherein each of said plurality of transmitting-receiving devices on the other parties comprises second input/output means, AV data receiving means, decrypting means, and second authenticating means, and

wherein said authenticating means performs a device authentication operation for mutually checking that both said devices are devices based on certain rules, and a key exchange operation for sharing a cryptographic key for simultaneously encrypting and decrypting the works when said transmitting-receiving device on another party with a history that authentication has been previously performed therefor is connected to a transmission line.

3. A works protecting system comprising an AV data transmitting-receiving device for transmitting contents of works and a transmitting-receiving device on another party for receiving the works,

wherein said AV data transmitting-receiving device comprises command input means, command control means, AV data transmitting means, encrypting means, first authenticating means, first input/output means, and device ID detecting means,

wherein said transmitting-receiving device on another party comprises second input/output means, AV data receiving means, decrypting means, and second authenticating means, and

wherein said authenticating means performs a device authentication operation for mutually checking that both said devices are devices based on certain rules, and a key exchange operation for sharing a cryptographic key for simultaneously encrypting and decrypting the works when said transmitting-receiving device on another party is connected to a transmission line.

4. A works protecting method for the works protecting system according to claim 1, said method comprising the steps of:

detecting an ID of said transmitting-receiving device on another party with said device ID detecting means;

checking whether the ID of said transmitting-receiving device on another party is included in historical information stored in said authentication histories storing means;

performing the device authentication operation and the key exchange operation with said second authenticating means on another party by said first authenticating means、 if the ID of said transmitting-receiving device on another party is included in the historical information;

notifying the command to said AV data transmitting means through said command control means and starting transmission of the AV data with said AV data transmitting means、 when a command input for an AV data transmission direction is provided from a user to said command input means;

waiting for a command input for an AV data transmission direction from a user to said command input means、 if the ID of said transmitting-receiving device on another party is not included in the historical information;

performing the device authentication operation and the key exchange operation with said second authenticating means on another party by said first authenticating means、 when the command input for the AV data transmission direction is provided;

recording the ID of said transmitting-receiving device on another party as historical information in said authentication histories storing means after the device authentication and the key exchange operations;

notifying the command to said AV data transmitting means through said command control means and starting transmission of the AV data with said AV data transmitting means;

encrypting the AV data with said encrypting means using the cryptographic key and sending the encrypted AV data to said first input/output means;

sending the encrypted AV data to a transmission line with said first input/output means;

receiving the encrypted AV data from the transmission line with said second input/output means;

decrypting the encrypted AV data with said decrypting means using the cryptographic key and sending the decrypted AV data to said AV data receiving means; and

receiving the decrypted AV data with said AV data receiving means.

5. A works protecting method for the works protecting system according to claim 2, said method comprising the steps of:

detecting an ID of said transmitting-receiving device on a first other party with said device ID detecting means;

checking whether the ID of said transmitting-receiving device on the first other party is included in historical information stored in said authentication histories storing means;

performing the device authentication operation and the key exchange operation with said second authenticating means on the first other party by said first authenticating means, if the ID of said transmitting-receiving device on the first other party is included in the historical information;

recording a cryptographic key shared as a result of the key exchange operation as a first cryptographic key in said cryptographic key storing means;

detecting an ID of said transmitting-receiving device on a second other party with said device ID detecting means;

checking whether the ID of said transmitting-receiving device on the second other party is included in historical information stored in said authentication histories storing means;

performing the device authentication operation and the key exchange operation with said second authenticating means on the second other party by said first authenticating means, if the ID of said transmitting-receiving device on the second other party is included in the historical information;

recording a cryptographic key shared as a result of the key exchange operation as a second cryptographic key in said cryptographic key storing means;

notifying the command to said AV data transmitting means through said command control means and starting transmission of the AV data with said AV data transmitting means, when a command input for an AV data transmission direction for said transmitting-receiving device on the first other party or for said transmitting-receiving device on the second other party is provided from a user to said command input means;

waiting for a command input for an AV data transmission direction for said transmitting-receiving device on the first other party from a user to said command input means, if the ID of said transmitting-receiving device on the first other party is not included in the historical information;

performing the device authentication operation and the key exchange operation with said second authenticating means on the first other party by said first authenticating means, when the command input for the AV data transmission direction is provided;

recording the ID of said transmitting-receiving device on the first other party as historical information in said authentication histories storing means after the device authentication and the key exchange operations;

recording a cryptographic key shared as a result of the key exchange operation as a first cryptographic key in said cryptographic key storing means;

waiting for a command input for an AV data transmission direction for said transmitting-receiving device on the second other party from a user to said command input means, if the ID of said transmitting-receiving device on the second other party is not included in the historical information;

performing the device authentication operation and the key exchange operation with said second authenticating means on the second other party by said first authenticating means, when the command input for the AV data transmission direction is provided;

after the device authentication and the key exchange operations, recording the ID of said transmitting-receiving device on the second other party as historical information in said authentication histories storing means;

recording a cryptographic key shared as a result of the key exchange operation as a second cryptographic key in said cryptographic key storing means;

notifying the command to said AV data transmitting means through said command control means and starting transmission of the AV data to the transmitting-receiving device on the first other party or to the transmitting-receiving device on the second other party with said AV data transmitting means;

encrypting the AV data with said encrypting means using the first cryptographic key and sending the encrypted AV data to said first input/output means, if the command input for the AV data transmission direction for said transmitting-receiving device on the first other party is provided from a user to said command input means;

sending the encrypted AV data to a transmission line with said first input/output means;

receiving the encrypted AV data from the transmission line with said second input/output means on the first other party;

decrypting the encrypted AV data with said decrypting means on the first other party using the first cryptographic key and sending the decrypted AV data to said AV data receiving means on the first other party; and

receiving the decrypted AV data with said AV data receiving means;

encrypting the AV data with said encrypting means using the second cryptographic key and sending the encrypted AV data to said first input/output means, if the command input for the AV data transmission direction for said transmitting-receiving device on the second other party is provided from a user to said command input means;

sending the encrypted AV data to a transmission line with said first input/output means;

receiving the encrypted AV data from the transmission line with said second input/output means on the second other party;

decrypting the encrypted AV data with said decrypting means on the second other party using the second cryptographic key and sending the decrypted AV data to said AV data receiving means on the second other party; and

receiving the decrypted AV data with said AV data receiving means.

6. The works protecting method for the works protecting system according to claim 4, wherein the transmission line for said AV data is IEEE1394 high-speed serial bus.

7. The works protecting method for the works protecting system according to claim 5, wherein the transmission line for said AV data is IEEE1394 high-speed serial bus.